“Access denied”? Managing access to the World Wide Web within the National Health Service (NHS) in England: technology, risk, culture, policy and practice

Catherine Ebenezer, Peter A Bath, Stephen Pinfield

Health Informatics Research Group, Information School, University of Sheffield, Sheffield, UK (lip12cme@sheffield.ac.uk)

“People assume that abusing the Internet is an IT problem … it isn’t an IT problem, it’s a management problem”. (Retired NHS IT manager)

The problem

Within the NHS in England there exist a variety of obstacles to professional information seeking, and to teaching and learning, apparently presented mostly by information governance, information security or other information technology-related policies and practices.

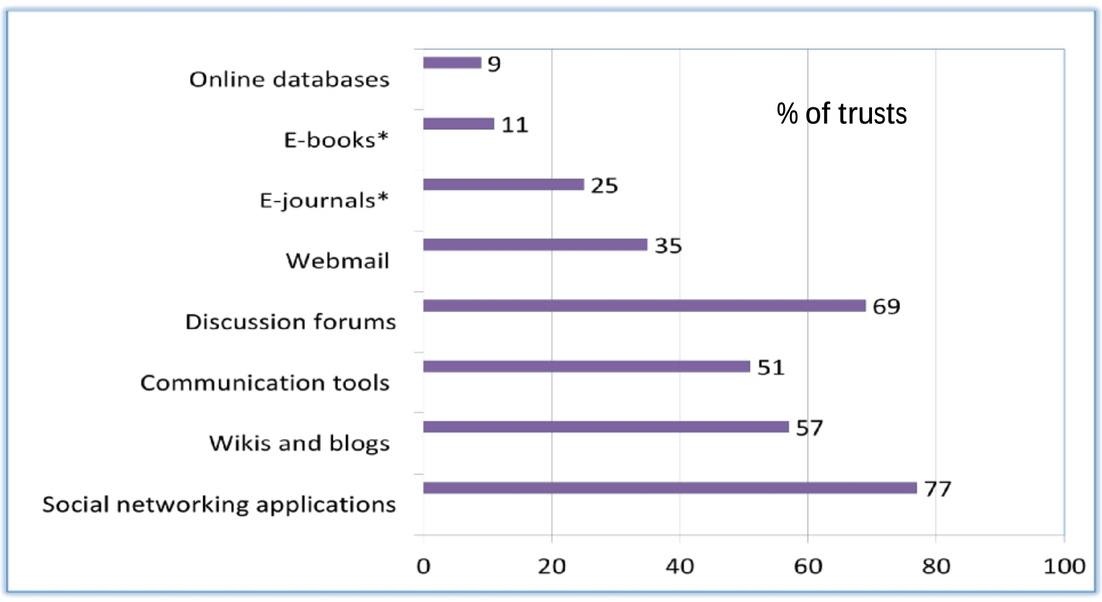
These obstacles, arising primarily at trust level, include the blocking of access to individual websites, or to whole categories of websites or web applications. The material blocked sometimes includes database and e-journal content purchased nationally or locally, and the websites of academic, governmental and professional bodies.

Hindrances to accessing the most current and up to date professional health information and, consequently, to the practice of evidence-based health care, in both clinical and managerial contexts, thereby appear to result, presenting potential risks to the quality of health services and health care provided. These exist both directly, in terms of unmet information need, and indirectly, in terms of organisational effectiveness, productivity and staff engagement.

Objectives

The main objectives of this study were to investigate:

1. The nature and extent of restrictions on access to the World Wide Web within NHS organisations
2. The impacts of these on professional information seeking and working practices
3. The attitudes, presuppositions and practices of information governance, IT, communications and human resources staff which bear on how IT infrastructures and web security are managed within NHS trusts, in relation to overall organisational priorities and strategies.



Online resources and applications blocked within NHS trusts
SHALL IT subgroup survey of NHS librarians (2008)

Methods

The study adopted a qualitative case study method, taking three NHS trusts of different types (district general hospital, mental health / community services, and teaching hospital) for its setting. The lead researcher [CE] conducted a total of 40 semi-structured interviews with library and workforce development staff, IT managers, information governance managers, and clinical professionals.

The researcher also interviewed a small number of key informants within national NHS information and e-learning services, and from among information security system vendors active within the NHS market.

A thematic analysis was undertaken. Interview findings were set in the context of the trusts’ and other relevant reports, policies, strategies and standards.

Results

Blocking of websites was a problem frequently reported by librarians to NICE. Very few instances of website blocking were reported within the district general hospital (DGH) and mental health services (MH); when a website had been incorrectly blocked, the IT department had unblocked the site promptly once the problem was reported. Staff in the teaching hospital trust (TH) experienced the greatest number of obstacles to information-seeking caused by the blocking of legitimate websites (‘false positives’); frequencies of blocking reported by clinical staff varied from ‘every two months’ to ‘constant’ or ‘daily, probably’. This affected the work of clinical educators in particular. Most of these blocked sites were not reported to the IT department. Whether or not staff members reported a blocked site appeared to depend upon their work pressures, the importance and uniqueness of the information sought, the time they anticipated that unblocking the site would take, and their previous experiences with the IT helpdesk.

Community-based staff were often based within non-NHS premises (e.g. local authority, general practice) and appeared more likely to be significantly disadvantaged by restrictive access control policies in force at these sites.

Much decision-making in relation to information security issues seemed to be tacit. IT security managers reported not having the time to evaluate the effectiveness or impact of the web security devices they deployed on NHS networks; they were dependent on reports from users (via calls logged with the trust helpdesk) of false positives. They were likely to accept the default configurations and categorisations of content offered by the suppliers. The IT manager at TH appeared aware (via emails sent to him) of the inconvenience caused to users by false positives. To a greater or lesser degree the main focus of attention and concern for him and his MH counterpart appeared to be on the potential security risks or impact on network traffic presented by ‘recreational’/ non-work use of the web.

Conclusions

To mitigate the potential security threat of so-called ‘malvertising’ (web-borne malware spread via syndicated advertising on websites), the teaching hospital trust had an explicit policy of blocking most advertising. This sometimes had the effect of blocking the entire site content. This was likely to have been a factor in the high number of blocked websites. Another possible factor may have been the trust secure web gateway’s lack of specificity in identifying and blocking inappropriate or compromised content.

Little attention has been paid within the NHS information systems community to the issue of access to legitimate published information. The focus is heavily on the secure and appropriate management of clinical records and systems. Information-seeking does not feature within professional cultures as an aspect of clinical or professional autonomy: there appears to be no value parallel with ‘academic freedom’ as understood within the higher education context. Hitherto there has been little or no strategic engagement between NHS IT and research dissemination or e-learning initiatives, either nationally or locally.

References

Blenkinsopp J. Bookmarks: web blocking – giving Big Brother a run for his money. He@lth Information on the Internet 2008; 62: 10-11.

Donaldson A, Walker P. Information governance--a view from the NHS. Int J Med Inform 2004; 73(3): 281–4.

Kolkowska E. Security subcultures in an organization – exploring value conflicts. In ECIS 2011 Proceedings, paper 237. http://aisel.aisnet.org/ecis2011/237

Provos N, Rajab M A, Mavromattis P. Cybercrime 2.0: when the cloud turns dark. ACM Queue 2009; 18: 46–53.

Technical Design Authority Group. TDAG survey of access to electronic resources in healthcare libraries. London: TDAG, 2009